Financité

FÉDÉRATION WALLONIE-BRUXELLES

ARNAQUES BANCAIRES

QUI EST RESPONSABLE ?

ANNE FILY & MORGANE KUBICKI - SEPTEMBRE 2025

Résumé

Un coup de fil de la « banque », un SMS pressant, un mail qui paraît officiel… et des milliers d'euros envolés. Chaque année, des milliers de Belges se font piéger par des arnaques bancaires de plus en plus sophistiquées. Derrière ces fraudes, de véritables organisations criminelles. Pourtant, lorsque les victimes contactent leur banque pour obtenir réparation, elles se retrouvent bien souvent face à une fin de non-recevoir, accusées d'avoir été négligentes en communiquant leurs données ou parfois même en réalisant le virement elle-mêmes.

Dans cette analyse, nous décrivons le mécanisme utilisé par les escrocs et la réponse des institutions bancaires. Nous abordons aussi la notion de négligence grave et le profil des victimes.

Introduction

L'année dernière, la tante de Dominique répond à un coup de téléphone de sa banque. L'employé lui demande son numéro de compte bancaire et ses codes d'accès. Elle donne tout… et se fait dépouiller de 50 000 euros. Elle porte plainte à la police, mais ne récupère presque rien du montant subtilisé par l'arnaqueur.

Quelques mois plus tard, le même scénario se répète. Cette fois-ci, le préjudice s'élève à 800 euros. Depuis placée sous tutelle administrative, elle ne dispose plus que d'un compte avec un peu d'argent de poche. Le préjudice est énorme *« et la banque a été infâme »*, insiste Dominique.

Vous avez probablement déjà reçu un mail qui vous demande de régler des frais postaux pour faire livrer votre colis bloqué à la douane, un SMS qui vous demande de renouveler votre carte, participé à un concours d'un site qui vous demandait étrangement beaucoup d'informations personnelles… Vous avez été prudent·e. Vous n'avez pas donné vos codes secrets ! Mais quelques semaines ou mois plus tard, un « employé » de votre banque vous appelle. Il possède beaucoup d'informations sur vos comptes et vous appelle justement parce que votre compte a été compromis. Ca ne peut pas être une arnaque…

1 13% des Belges ont déjà été victimes de phishing

Comme la tante de Dominique, des milliers de personnes se font avoir par ces arnaques bien ficelées. Selon une étude réalisée par la fédération du secteur financier avec le bureau d'études Indiville, 13 % des Belges ont déjà été victimes de phishing (se référer au lexique en page suivante) à un moment ou à un autre de leur vie. « *Beaucoup de gens tombent dans le piège et perdent de l'argent, entre 1 000 et 3 000 euros en général pour les cas de phishing. Avec la fraude à l'investissement, on recense moins de victimes mais de plus grosses sommes perdues. La moyenne est de 30 000 mais il y a des gens qui ont perdu 400 000* », détaille Katrien Eggers, responsable communication de la plateforme Safe on Web.

Selon les parquets correctionnels, le nombre de dossiers de recel et de blanchiment a triplé en dix ans. Après une légère baisse entre 2021 et 2023, le phénomène est reparti à la hausse. « *Cette recrudescence peut être rattachée principalement au phénomène des "money mules", ou mules financières, des personnes qui sont enrôlées par des organisations criminelles pour transférer de l'argent volé, par exemple à la suite d'un phishing, et qui prêtent à cet effet leur carte de banque, leur code et leur compte en banque à ces criminels* », précisent les parquets.

Mais les cas répertoriés ne constituent que la partie immergée de l'iceberg. « *Il y a un chiffre noir très important qui peut être dû à plusieurs facteurs : la honte de porter plainte, ne pas porter plainte parce qu'on considère que le préjudice est trop faible ou parce qu'on pense que la police ne pourra de toute façon rien faire* », note Christophe Axen, commissaire à la Computer Crime Unit.

2 Des organisations criminelles

Pourtant, *« Le plus souvent, nous sommes face à des organisations criminelles, pas de petits escrocs individuels »*, affirme le commissaire. La criminalité derrière un ordinateur, moins dangereuse, demande en effet d'avoir certaines compétences techniques. *« On constate une professionnalisation,* note Michel Rignanese, porte-parole du Centre pour la Cybersécurité Belgique (CCB). *Certaines*

personnes sont spécialistes pour rentrer dans une plateforme, puis revendre les données volées. Au final, ce sont des fichiers mis en vente et parfois reconstitués à partir de différentes sources. Il n'y a pas un grand groupe, ce sont différents groupes criminels. Cela reste du haut vol. »

Fin août, l'opérateur Orange annonce avoir été la cible d'une cyberattaque. 850 000 client·e·s sont concerné·e·s par cette fuite de données. Quelques heures plus tard, Testachats reçoit le témoignage d'une première victime contactée par un faux employé d'Orange et invitée à confirmer une opération via l'application Itsme.

La première étape est toujours celle du vol de données. Dans un deuxième temps, la victime est contactée par téléphone, généralement par un·e soi-disant employé·e de banque, qui prétend que des opérations suspectes ont eu lieu sur le compte du·de la client·e. On vous demandera d'agir vite, de faire un virement, de communiquer votre code secret. Tout cela est urgent. Récemment, on recense des cas ou le fraudeur (ou un de ses complices) se rend au domicile de la victime. Après un entretien sur la situation financière générale de celle-ci, la carte bancaire et le code PIN lui sont remis.

Lexique

PHISHING : « hameçonnage » en français, l'escroc vous arnaque en se faisant passer pour une autre organisation dans un mail qui ressemble à celui qui votre banque, service de livraison ou organisme public (par exemple) aurait pu vous envoyer.

PHISHING À LA CARTE BANCAIRE : l'escroc se fait passer pour votre banque qui vous invite à remplacer votre carte de débit. Il vous est alors demandé de compléter vos données personnelles et d'envoyer votre « ancienne » carte par la poste.

SMISHING : même technique que le phishing à la différence que ce sont des SMS ou messages Whatsapp qui sont envoyés.

VISHING : hameçonnage par téléphone.

SPOOFING : regroupe les pratiques de phishing et smishing.

FRAUDE À L'INVESTISSEMENT : proposer un investissement avec un rendement très intéressant. Il s'avère par la suite que l'investissement en question n'existe pas ou qu'il rapporte bien moins que prévu

BOILER ROOM : l'escroc vous propose d'acheter des actions ou autres produits financiers, mais la plateforme d'investissement est frauduleuse. Cette arnaque soumet la victime à une forte pression de verser plus d'argent (d'où l'appellation anglaise de « boiler room ») mais l'argent n'est jamais récupéré.

RECOVERY ROOM : vous avez été victime d'une arnaque et on vous appelle pour vous aider à récupérer votre argent. L'escroc est alors souvent lié à l'arnaque précédente et demande à nouveau de l'argent qui ne sera pas reversé.

MULE FINANCIÈRE : utilisée pour servir d'intermédiaire. Il s'agit souvent de jeunes qui « prêtent » leur compte un certain temps pour que l'argent leur soit envoyé puis transféré sur d'autres comptes rapidement.

3 C’est déjà trop tard

Dans le cas de Maryam, arnaquée par un faux conseiller bancaire, l’escroc lui demande de confirmer un virement de 20 000 euros via l’application Itsme. Et avant de raccrocher, rigole en la remerciant pour sa collaboration ! Elle contacte immédiatement sa banque, mais il est trop tard. *« J’espérais que Beobank m’aiderait, mais je n’ai reçu aucun soutien »*, déplore-t-elle au Het Laatste Nieuws. Sa banque ne la rembourse qu’en partie, invoquant une responsabilité partagée.

Maryam aurait-elle pu annuler son virement ? Non. *« La possibilité d’annuler un paiement introduit une incertitude juridique pour le·la bénéficiaire, qui ne peut plus être sûr de recevoir les fonds. Cela pose des problèmes dans des transactions courantes, comme par exemple, pour l’achat de voitures d’occasion ou sur les marchés aux puces »*, justifie Febelfin, la fédération du secteur financier.

En réalité, il existe bien une procédure qui permet à la banque de la victime de demander à une autre banque de bloquer les fonds transférés de manière frauduleuse, mais seulement dans le cas de « mules financières ». Dans le cadre des arnaques, les criminels font souvent appel à des mules pour recevoir l’argent à leur place, afin de préserver leur anonymat. *« Il s’agit d’un protocole interbancaire permettant à la banque de la victime de demander à la banque de la mule financière de récupérer les sommes détournées. Toutefois, cette procédure n’a pas de caractère obligatoire »*, précise Charline Gorez, porte-parole de Febelfin.

En dehors de cette exception, une banque ne peut pas bloquer un transfert d’argent sans réquisition d’un magistrat. Une procédure bien trop lente pour éviter de voir l’argent s’évaporer. *« Le travail d’enquête de la police est de suivre l’argent. Malheureusement, ces sommes bougent très vite. Elles passent par d’autres comptes qui séparent le montant en plusieurs transactions puis sont souvent converties en cryptomonnaie »*, pointe Christophe Axen, qui ajoute que la collaboration avec les banques est loin d’être rapide.

4 Les banques peu coopératives

Il existe bien dans les banques des systèmes pour suspendre une transaction considérée comme suspecte. Mais certain·e·s fraudeur·euse·s connaissent visiblement les systèmes de détection et font tout pour passer entre les mailles du filet en faisant, par exemple, dix virements de 499 euros en moins d’une heure.

Ce qui est certain, c’est que ce sont dans les cas de phishing que les banques sont le moins coopératives. En 2024, 82 % des dossiers arrivés sur la table du médiateur financier se sont clôturés sur une note positive. Mais ce pourcentage est poussé à la baisse par les dossiers de phishing où le taux de réussite n’est que de 37,5 % (contre 98 % dans les autres désaccords).

Car les banques accusent les victimes d’avoir été négligentes en communiquant leurs données ou parfois même en réalisant le virement elle-mêmes. « La définition de la négligence grave n’est pas la même selon que vous demandez aux banques ou au service de médiation », précise Jean Cattaruzza, médiateur des services financiers (lire plus dans l’encadré en page suivante)

En Belgique, la jurisprudence n’offre pas de réponse claire sur la responsabilité des client·e·s dans ce type d’arnaque et le remboursement que doivent opérer les banques. D’autres pays sont plus clairs sur la question. En Grèce, les banques ont eu le choix d’investir dans un système de détection de la fraude ou d’indemniser les victimes même en cas de négligence grave.

Concrètement, la perte est partagée entre le·la consommateur·rice et le prestataire de services de paiement, sauf si la banque peut prouver qu'elle a mis en place des mécanismes de contrôle supplémentaires et efficaces. Outre-manche, toutes les entreprises proposant des services de paiement doivent rembourser les consommateur·rice·s victimes d'arnaque. Depuis octobre 2024, sauf si la victime a ignoré l'avertissement de la banque indiquant que le paiement était probablement frauduleux, elle est remboursée dans les 5 jours ouvrables jusqu'à
85 000 livres (98 000 euros).

5 Que dit la réglementation ?

La législation qui s'applique à la sécurité de nos transactions de paiement est d'origine européenne. La directive sur les services de paiement adoptée en 2015 (PSD2) a été transposée en droit belge en 2018.

Cette législation avait notamment pour objectif de mieux protéger les consommateur·ice·s face aux risques de sécurité accrus liés aux paiements électroniques. C'est cette législation qui a notamment introduit le principe de l'authentification forte lorsque l'on consulte son compte en ligne ou que l'on initie un paiement électronique en ligne. On commence par s'identifier, puis on autorise l'opération.

Concrètement, il nous est demandé d'utiliser deux des éléments suivants :

- quelque chose que l'on connaît (ex. : un mot de passe, un code pin, une question secrète) ;
- quelque chose que l'on possède (ex. : une carte de paiement, un smartphone, un digipass, une clé USB d'authentification) ;
- quelque chose qui nous est propre (ex. : une empreinte digitale, une reconnaissance vocale, la forme de l'iris).

Si l'on est victime d'une opération débitée sur notre compte bancaire qui n'a pas été vérifiée par notre banque par l'authentification forte, la banque est tenue de rembourser le montant dérobé à son·sa client·e. L'opération est réputée non autorisée.

En revanche, il n'y a pas droit au remboursement si le·la titulaire du compte a commis une négligence grave au moment du paiement ou si il·elle a commis une fraude.

À partir du 9 octobre 2025, une nouvelle législation européenne rend obligatoire la vérification de la correspondance entre le nom du bénéficiaire du paiement et le numéro de compte (IBAN) pour tous les virements en euros. Les banques devront fournir une alerte en cas de non-concordance, permettant aux client·e·s de valider ou d'annuler le virement en toute connaissance de cause. Cette mesure vise à réduire la fraude et les erreurs dans les paiements. Quelques banques n'ont pas attendu la dernière minute pour mettre en place cette nouvelle obligation : Argenta, KBC et BNP Paribas Fortis pour les virements faits à partir de son application.

Négligence grave

Pour ne pas avoir à dédommager les client·e·s victimes d'arnaque, les banques évoquent généralement la négligence grave.

La victime n'aurait pas été suffisamment prudente, des signaux « évidents » lui permettaient de deviner qu'il·elle se faisait avoir. Dans les faits, il appartient à la banque concernée de démontrer qu'il y a eu négligence grave de la part de son·sa client·e. Car la notion de négligence grave n'est pas définie par la législation. Les institutions financières ont une interprétation relativement large de cette notion. Elles assimilent l'autorisation au consentement et considèrent qu'à partir du moment où la victime a fait usage de l'authentification forte (lire ci-dessus), elle a elle-même autorisé le virement. Conséquence : elle a fait preuve d'une négligence grave.

Pour l'Ombudsfin, Il faut analyser le degré d'implication de la victime dans le processus de fraude et le degré de sophistication de ladite fraude. Or, si les récits des escrocs sont vraisemblables dans le chef des victimes, il est difficile d'envisager qu'il y ait eu négligence grave. Les techniques des fraudeur·euse·s se professionnalisent d'année en année et excellent parfois à surfer sur les émotions de leurs victimes pour arriver à leurs fins. *« Cela ne sert à rien de définir la négligence grave, car avec l'évolution des techniques des escrocs, cette définition devient rapidement obsolète »*, pense cependant Jean Cattaruzza.

Il s'agit aussi de vérifier si la banque n'a pas failli à détecter la fraude. Dans plusieurs dossiers introduits chez le médiateur, il a été démontré que le fraudeur a réussi à confirmer de nombreuses transactions sans être remarqué par les systèmes de détection de fraude de la banque (ou remarqué trop tardivement). Malheureusement, les banques ont rarement tenu compte de ces éléments pour intervenir même partiellement dans le remboursement de la victime.

6 Ça n'arrive pas qu'aux autres

En août 2021, un homme reçoit un appel de sa banque, c'est le bon numéro qui s'affiche. Un conseiller lui apprend que quelqu'un essaie d'effectuer avec sa carte bancaire un paiement de 9 000 euros dans une bijouterie à Madrid. Cet homme confirme que ce n'est pas lui. Pour bloquer le paiement, le conseiller lui demande de confirmer des informations personnelles et mentionne même les dernières transactions qu'il a effectuées. Pour cela, le conseiller lui demande de valider un code qui vient de lui être envoyé. Sans le savoir, il venait de valider l'achat de ce bijou. Cet homme, c'était Dominique Strauss-Kahn. Désormais plus connu pour être accusé d'agressions sexuelles que pour sa carrière politique, l'homme a tout de même été à la tête du Fonds monétaire international et ministre de l'Économie et des finances en France.

À l'époque, ce type de fraude était moins courant, mais il montre qu'il peut toucher tout le monde. *« Ce que l'on sait des victimes, c'est que cela n'a rien à voir avec le niveau d'éducation. Statistiquement par contre, il est vrai qu'il y a plus de personnes âgées »*, affirme Jean Cattaruzza, le médiateur des services financiers.

« En ce qui concerne la fraude à l'investissement, la plupart des victimes ont la quarantaine. Le deuxième groupe le plus touché est les jeunes. Pour les autres types d'arnaques, il n'y a pas vraiment de profil. Tout le monde peut potentiellement être victime », précise Katrien Eggers, responsable de la

communication du Centre pour la cybersécurité Belgique.

Selon Nathalie Granier, psychologue, analyste et spécialiste des contenus cyber, l'escroc va faire appel à deux concepts psychologiques pour manipuler ses victimes et leur faire faire quelque chose qu'elles n'auraient pas faites en temps normal. D'abord, la psychologie comportementale. Cela peut être la mise en place d'un environnement bruyant, stressant ou le plus souvent dans le cas de phishing la création d'un sentiment d'urgence. La peur qui entraîne un pic de stress aigu induit une vigilance diminuée. Trop de sollicitations, lorsqu'il nous est demandé de réaliser beaucoup d'opérations, vont nous mener à se focaliser sur une tâche et oublier la sécurité. Si à cela s'ajoute un contexte propre à la victime qui peut être distraite par son environnement au moment de l'appel le vendredi soir plutôt que le matin d'un jour de semaine, la victime est particulièrement vulnérable.

Vient ensuite la psychologie cognitive. Il s'agit des facteurs émotionnels, un ensemble de leviers psychologiques qui peuvent être exploités pour influencer ou manipuler une personne afin d'obtenir des informations ou une coopération. Nous sommes tou·te·s sujet·te·s à des préjugés. Nous avons tendance à faire confiance aux messages émanant de personnalités importantes, d'institutions ou de personnes que nous connaissons. Un·e utilisateur·rice peut rencontrer un avertissement de sécurité lors de la navigation sur un site web, mais au lieu de prendre cette alerte au sérieux, il·elle le considère comme une fausse alarme ou une erreur du navigateur. Enfin, de nombreuses personnes peuvent faire preuve d'un excès de confiance, pensant qu'elles ne tomberont jamais dans une arnaque.

Les enquêtes montrent également qu'un certain nombre de client·e·s utilisent la banque en ligne sans se sentir à l'aise. *« On est pas formé·e·s au digital, ça nous tombe dessus et on doit se débrouiller. C'est une évaluation que le monde bancaire doit faire par rapport à ses client·e·s »*, regrette Michel Rignanese. Alors qu'une opération réalisée en agence relève de la responsabilité de la banque, une transaction autorisée en ligne est celle du·de la client·e.

Recommandations Financité

En lien avec cette analyse, le mémorandum Financité *« 52 propositions pour une finance au service de l'intérêt général, proche et adaptée aux citoyen·ne·s »* [1] plaide pour.

Les banques disposant du monopole des dépôts de par la loi, elles ont en contrepartie des obligations de service vis-à-vis de leur clientèle. Que l'on habite dans une commune pauvre ou riche, rurale ou urbaine, tout le monde devrait donc pouvoir accéder à un service bancaire de proximité qu'il faudrait inscrire dans la loi bancaire sur la base des principes suivants :

- une distance maximale à parcourir prenant en compte les différents moyens d'accès des personnes « non digitalisées » ;
- des solutions variées prenant en compte les besoins de la population : agence fixe, agence mobile, visites à domicile, etc ;
- des services bancaires par téléphone dans toutes les banques afin de pouvoir au minimum effectuer des virements et connaître la situation de son compte ;
- un véritable service téléphonique d'aide avec accès direct à des employé·e·s (et non un centre d'appels automatisé) spécialement formés à l'écoute, qui pourront répondre aux questions des personnes confrontées à des difficultés. Ces employé·e·s devraient disposer d'un temps raisonnable pour répondre aux questions.
- Prévoir des sanctions dissuasives contre les banques qui ne remboursent pas immédiatement leurs clients victimes de fraude qui n'ont commis aucune faute.
- Mise en place au niveau européen d'un contrôle nom-IBAN pour limiter les fraudes.

[1] Mémorandum Financité 2024 / https://www.financite.be/fr/news/decouvrez-notre-memorandum-en-vue-des-elections-2024

A propos de Financité

Si vous le souhaitez, vous pouvez nous contacter pour organiser avec votre groupe ou organisation une animation autour d'une ou plusieurs de ces analyses.

Cette analyse s'intègre dans une des 3 thématiques traitées par le Réseau Financité, à savoir :

Finance et société :
Cette thématique s'intéresse à la finance comme moyen pour atteindre des objectifs d'intérêt général plutôt que la satisfaction d'intérêts particuliers et notamment rencontrer ainsi les défis sociaux et environnementaux de l'heure.

Finance et individu :
Cette thématique analyse la manière dont la finance peut atteindre l'objectif d'assurer à chacun, par l'intermédiaire de prestataires « classiques », l'accès et l'utilisation de services et produits financiers adaptés à ses besoins pour mener une vie sociale normale dans la société à laquelle il appartient.

Finance et proximité :
Cette thématique se penche sur la finance comme moyen de favoriser la création de réseaux d'échanges locaux, de resserrer les liens entre producteurs et consommateurs et de soutenir financièrement les initiatives au niveau local.

Depuis 1987, des associations, des citoyen·ne·s et des acteurs sociaux se rassemblent au sein de Financité pour développer et promouvoir la finance responsable et solidaire.

L'ASBL Financité est reconnue par la Communauté française pour son travail d'éducation permanente.